AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Austin Love, Special Agent of the Drug Enforcement Administration ("DEA"), being duly sworn, hereby state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am an investigative or law enforcement officer of the United States, within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516 of Title 18, United States Code. I am further authorized to execute and serve search warrants under Title 21, United States Code, Section 878.

2. I am a Special Agent with the Drug Enforcement Administration ("DEA") and have been so employed since January 2012. I am currently assigned to the DEA Miami Field Division, Counternarcotic Cyber Investigations Task Force, which is responsible for investigations where computers, networks, telecommunication devices, and other technological instruments are the vehicle for the distribution of illegal drugs and/or drug-sale proceeds.

3. Prior to my employment with the DEA, I was employed for approximately three years with the Department of Homeland Security, U.S. Customs and Border Protection, Office of Field Operations where I was a Customs and Border Protection Officer in San Francisco, California.

4. I have received training in the enforcement of laws regarding controlled substances, as found in Title 21 of the United States Code. I have attended the DEA's sixteen-week basic agent training academy in Quantico, Virginia, where I received specialized training in the methods and techniques used by individuals involved in drug trafficking. I have conducted drug-trafficking and money laundering investigations and I have debriefed and participated in the debriefings of defendants, informants, and witnesses who have participated in drug-trafficking activity.

5. Through my training and experience, I have familiarized myself with the methods employed by drug traffickers in general to smuggle, safeguard, and distribute drugs, and to collect and launder drug-related proceeds. These methods, which are made in an attempt to avoid detection by law enforcement and to circumvent drug trafficking investigations, include the use of use of coded or vague communications, cellular telephones, computers, false or fictitious identities, counter-surveillance, and sophisticated schemes tied to legitimate businesses, to name a few.

II. PURPOSE OF AFFIDAVIT

6. This Affidavit is made in support of an application for a search warrant for room number 133 of the WoodSpring Suites Nashua Merrimack located at 2 Executive Park Drive, Merrimack, New Hampshire 03054 (the "TARGET LOCATION"), as described more fully in Attachment A. The requested search warrant seeks authorization to seize evidence, contraband, fruits of crime, other items illegally possessed, and property designed for use, intended for use, or used in committing , violations of Title 21, United States Code, Section 846 (Conspiracy to Distribute a Controlled Substance), Section 841 (a)(1) (Distribution of a Controlled Substance), and Title 18, United States Code, Section 1956 (h) (Conspiracy to Commit Money Laundering), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

7. The facts set forth in this Affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This Affidavit is intended to show that there is sufficient probable cause for the requested warrant, and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this Affidavit are related in substance and in part only.

III. FACTS SUPPORTING PROBABLE CAUSE

8. This application stems from an ongoing criminal investigation into vendors who facilitate drug trafficking occurring on the dark web.[1] Dream Market is one of many criminal marketplaces operating on the dark web.[2] From 2013 to present day, Dream Market has facilitated the anonymous sale of illegal items, such as controlled substances, in exchange for bitcoin and other, peer-to-peer crypto-currencies (also known as, virtual currencies).

9. Starting in January 2018, DEA agents viewed the profile of 5thAvenue, a Dream Market vendor. 5thAvenue advertised the sale of heroin and MDMA. From February 13, 2018 through February 26, 2018, agents periodically reviewed 5thAvenue's active listings and captured screen shots. During this time, 5thAvenue had active listings for: heroin – 1 gram (11 product ratings), heroin – ¾ gram (10 product ratings), heroin - .25 gram (11 product ratings), 100 mg MDMA capsules (0 product ratings).[3] The total amount of heroin sold during this time is approximately 21.25 grams.

10. On June 1, 2018, DEA agents conducted an undercover purchase of four "Sacks 5thAvenue Dime Bags #3 Heroin NO LIMIT" from 5thAvenue. The vendor posted that one dime bag[4] was for sale for .0014 Bitcoin (approximately $10.40). Thus, four dime bags and shipping would come to a total .00627 Bitcoin (approximately $46.60). Payment was to be made through the Dream Market escrow system. The agents provided the vendor with an undercover post office box address located in Miami-Dade County, Florida. On June 11, 2018, DEA agents received a

[1] The dark web is a subsection of the deep web which is part of the world wide web that is not indexed by traditional search engines. The dark web requires specific software, configurations or authorizations to access. Identities and locations of darknet users remain anonymous due to a layered encryption system.
[2] Public sources define Dream Market as founded in 2013 and is the oldest operational darknet market.
[3] A customer can only leave a product rating if they are a confirmed buyer by Dream Market administrators. Therefore, each product rating is equivalent to one known sale.
[4] A dime bag equals one-tenth of a gram of heroin.

package in the undercover USPS mailbox from "Patty O'Niel, 191 Indian Rock Rd, Merrimack, NH 03054." This package was sent via Priority Mail and listed a tracking number of 9505 5158 4518 8153 2294 80. Inside the package was .3530 grams of heroin. DEA laboratory results confirmed it was heroin with 41% purity.

11. On June 2, 2018, 5thAvenue informed the buyer (DEA agents), via email, that its account was hacked and that no payment should be sent until further notice. No instructions for payment were ever sent by 5thAvenue and subsequently no payment has ever been made for this heroin transaction.

12. U.S. Postal Inspectors identified the debit card number (and corresponding bank) that was utilized to purchase the postage associated with tracking number 9505 5158 4518 8153 2294 80. Subpoenaed bank records from TD Bank revealed that Brian Knight (hereinafter "Knight") was the sole account holder of the debit card used to purchase the postage. ATM photographs were also obtained pursuant to the subpoena which show a male and a female using the debit card issued to Knight at an ATM. The male can also been seen driving a gold Jeep Grand Cherokee in these photos. The subpoenaed bank records from TD Bank also show multiple charges using the debit card to WoodSpring Suites in Merrimack, New Hampshire. I have compared known photographs of Brian Knight and Tina Kearns (hereinafter "Kearns") to the images of the individuals depicted in the subpoenaed photographs and the individuals match the known photographs. I have also reviewed records from the Massachusetts Registry of Motor Vehicles, and those records establish that a Jeep Grand Cherokee is registered to Kearns.

13. The packaging for the heroin received on June 11, 2018 was submitted for fingerprint analysis to the DEA laboratory. One latent print of value was identified from the silver Ziploc bag that was part of the interior packaging for the heroin. This print was a match for Brian

Knight.

14. Sometime in late July 2018, DEA agents obtained the guest list for the WoodSpring Suites Nashua Merrimack. These records show that Knight and Kearns are currently residing in room 133 (the TARGET RESIDENCE). Knight and Kearns' reservation is confirmed through August 29, 2018. Beginning around July 20, 2018, surveillance of the TARGET LOCATION revealed Knight and Kearns accessing the TARGET LOCATON. Surveillance has continued and Knight and Kearns are still accessing the TARGET LOCATION.

15. On July 12, 2018, a new vendor account was created on Dream Market with the name "Sacks_5thAvenue." Sacks_5thAvenue advertised that they were formerly the vendor 5thAvenue on Dream Market. Agents determined that the product listings for Sacks_5thAvenue were nearly identical to those of 5thAvenue.

16. On July 31, 2018, DEA agents conducted an undercover purchase from Sacks_5thAvenue. Agents purchased four units of "3/4 Gram Pure Afghan #3 Base Heroin (Fent Free)" for .00944 Bitcoin per unit. Agents also paid for USPS Priority Shipping, which totaled .03907 Bitcoin (approximately $301.20) for both the heroin, and shipping. Payment was made through the Dream Market escrow system. The agents provided the vendor with the same undercover post office box address used for the June 1, 2018 purchase of heroin. On August 14, 2018, agents received a package in the undercover USPS mailbox from "Energy Concepts, 94 Indian Rock Rd, Merrimack, NH 03054." This package was sent via Priority Mail but did not have a tracking number. Inside the package was approximately 3.25 grams of a powder material. Laboratory testing confirmed the material was heroin. On that same day, after confirming receipt of the suspected heroin, DEA agents finalized the transaction, that is, the bitcoin was released from the Dream Market escrow to the vendor, Sacks_5thAvenue.

17. On August 8, 2018, an anonymous tip was received by the Merrimack Police Department Web Tip Line. The tipster stated that Knight is currently living in WoodSpring Suites Room 133, Merrimack. The tipster stated that Knight told the tipster that he (Knight) and his wife, Tina, are running an online drug business and use the USPS to send the drugs to customers. The tipster stated that Knight also utilizes meth, heroin, and other drugs. Knight also told the tipster that Knight is cooking meth in room 133 at the WoodSpring Suites.[5] The tipster stated that Knight drives a gold jeep Cherokee.

18. Based on my training and experience, combined with the evidence gathered from this investigation, I believe that Knight is operating his narcotic sale business from the TARGET LOCATION. I believe that Knight cuts, weighs and packages narcotics inside the TARGET LOCATION. I also believe that he utilizes computers and/or other digital devices to access the dark web marketplace, Dream Market. Based in part on the surveillance in this case, I believe that Knight is accessing his digital devices, and therefore Dream Market, while inside the TARGET LOCATION.

IV. TRAINING AND EXPERIENCE REGARDING DRUG TRAFFICKING OFFENSES

19. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug traffickers often store documents and other items relating to the possession, manufacture, importation, exportation and distribution of drugs and to the illegal proceeds of drug trafficking where they are residing, including hotels rooms if that is their primary temporary residence, where they are readily available and concealed from law enforcement.

[5] On August 8, 2018, law enforcement in New Hampshire went to the TARGET LOCATION to check for the smell of chemicals for the safety of the residents in the hotel. No odor was detected. However, all other information provided by the anonymous tipster has been corroborated.

These documents and items include invoices, shipping labels, tracking numbers, boxes, and envelopes.

b. Drug traffickers commonly store drugs and drug paraphernalia, including packaging materials, cutting agents, and manufacturing tools, in their where they are residing, including hotels rooms if that is their primary temporary residence, where they are readily available and concealed from law enforcement.

c. Drug traffickers attempt to mask the distinct odors of particular drugs through the use of heat sealing and canning devices or aromatic substances such as laundry soap, dryer sheets, air fresheners, or axle grease. Drug traffickers also use several packaging layers when shipping drugs to decrease the odor.

d. Drug traffickers keep books, receipts, notes, ledgers, and other records relating to their drug distribution activities. Because drug traffickers often "front" drugs to their customers - that is, sell the drugs on credit - or receive drugs from their suppliers on credit, such records are necessary to keep track of the amounts paid and owed by/to their customers and suppliers. These ledgers are more commonly known as "pay/owe sheets," and may be as simple as notations on miscellaneous pieces of paper or may be recorded more formally in notebooks or even computer spreadsheets. "Pay/owe sheets" are frequently encoded in order to protect the identities of customers and suppliers. Drug traffickers often keep such records where they are residing, including hotels rooms if that is their primary temporary residence,

e. Drug traffickers commonly keep large sums of currency, financial instruments, precious metals, jewelry, gift cards, and other items of value, which either are the proceeds from drug sales or are intended for the purchase of drugs. When drug traffickers amass such wealth, they often attempt to conceal it and its origin from discovery by law enforcement.

Drug traffickers use many different techniques to do so, including using digital currency, and using savings and checking accounts, securities, cashier's checks, money drafts and letters of credit to exchange drug proceeds into money that appears to come from a legitimate source. Drug traffickers also use drug proceeds to purchase real estate or cars, and establish shell corporations and business fronts that they use to launder drug proceeds. Drug traffickers often use fictitious or "straw-holder" owners to conceal the true ownership of real estate, cars, or other valuable items purchased with the proceeds of drug sales. In addition, drug traffickers often use wire transfers, cashier's checks, and money orders to pay for drugs or other costs relating to their distribution activities. Drug traffickers often keep these items of value, and records relating to them, where they are residing, including hotels rooms if that is their primary temporary residence, where they are readily available and concealed from law enforcement.

f. Drug traffickers go to great lengths to hide and secure the drugs, drug proceeds, other items of value, and records relating to their drug business. This is to safeguard those items against robbery and keep them hidden from law enforcement. Drug traffickers hide these items by storing them in secure locations, including safes, vaults, or other locked containers.

g. Drug traffickers often use USPS or commercial express mail delivery companies, such as FedEx or UPS, to ship drugs and money throughout the United States. They do so, at least in part, because of the convenience of the service, the availability of internet and phone tracking services, the speed of delivery, and to reduce their risk of arrest during the transportation of drugs from one place to another. They often use hand-written air bills, drop the packages near closing time, pay for such services in cash, and use fictitious names, addresses, and telephone numbers to avoid detection by law enforcement. Drug traffickers frequently keep records relating to their use of these services, such as receipts, copies of air bills, empty and

previously used boxes, packing tape, packaging materials, and package tracking records printed from the internet, where they are residing, including hotels rooms if that is their primary temporary residence, where they are easily available for reference.

h. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. These persons frequently maintain listings of names, aliases, telephone numbers, pager numbers, facsimile numbers, physical addresses, and email addresses, sometimes encoded and sometimes not encoded, for the purpose of contacting their suppliers, customers, transporters, and others involved in their illicit drug distribution activities. These records are typically maintained where they are residing, including hotels rooms if that is their primary temporary residence, where they are readily available and concealed from law enforcement. Moreover, such records are often stored electronically within the memory of telephones, computers, and personal digital assistants such as iPhone and Blackberry devices.

i. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds. Documents relating to such travel, such as calendars, travel itineraries, maps, airline tickets, baggage stubs, frequent use club membership information, airline, rental car, and hotel receipts, credit card bills, photographs, videos, passports, and visas, are often kept by drug traffickers where they are residing, including hotels rooms if that is their primary temporary residence, where they are readily available.

j. Drug traffickers frequently possess firearms, ammunition, silencers, explosives, incendiary devices, and other dangerous weapons to protect their profits and supply

of drugs from others who might attempt to forcibly take such items and harm the drug traffickers during transactions. Such weapons, which are often stolen or otherwise possessed illegally, are typically kept where they are residing, including hotels rooms if that is their primary temporary residence, where they are concealed from law enforcement and readily available.

k. Drug traffickers often use two-way radios, police scanners, video surveillance systems, and other counter surveillance equipment to prevent detection by law enforcement. Such items are typically kept where they are residing, including hotels rooms if that is their primary temporary residence.

l. Drug traffickers frequently take, or cause to be taken, photographs and videos of themselves, their criminal associates, their real and personal property, their weapons, and their drugs. Such items are often stored where they are residing, including hotels rooms if that is their primary temporary residence, and on digital devices.

m. Drug traffickers often use electronic devices such as cellular telephones, satellite telephones, pagers and text messaging devices, voicemail or answering machine systems, telephone calling cards, computers, tablets, email, and personal digital assistants such as iPhone and Blackberry devices in order to communicate with their suppliers, customers, transporters, and others involved in their illicit drug distribution activities. Drug traffickers often keep the documents and records described above on those devices. Drug traffickers often use multiple phones, including not only their own phones but also phones of family members and significant others, in order to avoid detection by law enforcement. Drug traffickers often keep these devices where they are residing; including hotels rooms if that is their primary temporary residence, where they are readily available.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

20. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

21. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

22. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are

designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

23. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500-gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

24. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically

downloaded into a temporary directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

25. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created

and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

26. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

27. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not

scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

28. As discussed herein, based on my training and experience I believe that digital devices will be found during the search. I know from my training and experience and my review of publicly available materials that Apple Inc., Motorola, HTC, and Samsung, among other companies, produce devices that can be unlocked by the user with a numerical or an alpha-numerical password, or, for some newer versions of the devices, with a fingerprint placed on a fingerprint sensor. Each company has a different name for its fingerprint sensor feature; for example, Apple's is called "Touch ID." Once a user has set up the fingerprint sensor feature in the security settings of the device, the user can unlock the device by placing a finger or thumb on the device's fingerprint sensor. If that sensor recognizes the fingerprint or thumbprint, the device unlocks. Most devices can be set up to recognize multiple prints, so that different prints, not necessarily from the same person, will unlock the device. In my training and experience, users of devices with a fingerprint sensor feature often enable that feature, because it unlocks the phone more quickly than the entry of a passcode or password but still offers a layer of security.

29. In some circumstances, fingerprint sensors will not work, and a passcode must be entered to unlock the device. For example, with Apple, Touch ID will not work if (1) more than 48 hours have passed since the device has been unlocked, (2) the device has been turned on or restarted, (3) the device has received a remote lock command, or (4) five attempts to match a fingerprint have been unsuccessful. Other brands have similar restrictions. I do not know the passcodes of the devices likely to be found at the TARGET LOCATION.

30. For these reasons, while executing the warrant, agents will likely need to use the

fingerprints or thumbprints of any user(s) of any fingerprint sensor-enabled device(s) to attempt to gain access to that device while executing the search warrant. The warrant seeks the authority to compel the use of the fingerprint and/or thumbprint of every person who is located at the TARGET LOCATION during the execution of the search and who is reasonably believed by law enforcement to be a user of a fingerprint sensor-enabled device that is located at the TARGET LOCATION and falls within the scope of the warrant. The government may not be able to obtain the contents of the devices if those fingerprints are not used to access the devices by depressing them against the fingerprint sensor at the time of the search. Although I do not know which of the fingers are authorized to access on any given device, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for fingerprint sensors, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode or password.

31. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VI. CONCLUSION

32. Based on the foregoing, there is probable cause to believe that the evidence, fruits, and instrumentalities of the offenses described in Attachment B will be found at the TARGET LOCATION described in Attachments A.

/s/ Austin Love
Austin Love, Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me on August, 27, 2018, in Concord, New Hampshire.

HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE